BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Pada era teknologi informasi saat ini masalah keamanan pada komputer atau pun sistem komputer menjadi isu penting. Masalah keamanan sering kali kurang mendapat perhatian dari para pengguna teknologi informasi. Apalagi saat ini banyak masyarakat bergantung pada komputer untuk menciptakan, menyimpan dan mengatur informasi-informasi penting, seperti halnya informasi diri, keuangan, informasi perusahaan,dan sebagainya. Maka sebagai pengguna teknologi informasi perlu melindungi komputer dan data agartidak hilang, rusak, ataupun disalahgunakan.

Pengiriman dan penyimpanan pesan melalui media elektronik juga sudah banyak dilakukan. Untuk menjaga keamanan dan keutuhan data tak jarang data tersebut perlu dirahasiakan. Kriptografi merupakan dasar untuk memahami keamanan pada komputer dan juga kerahasiaan informasi. Metode yang digunakan untuk mengamankan data ada bermacam-macam. Metode–metode kriptografi tersebut mempunyai teknik dan cara tersendiri. Langkah–langkah pengerjaan setiap metode pun berbeda–beda, baik dari segi panjang maupun kerumitan. Begitu pentingnya kriptografi untuk keamanan informasi, sehingga jika berbicara mengenai masalah keamanan yang berkaitan dengan penggunaan komputer, maka orang tidak bisa memisahkannya dengan kriptografi.

Kriptografi merupakan seni dan ilmu menyembunyikan informasi dari penerima yang tidak berhak. Ilmu kriptografi perkembangannya juga sangat cepat. Membicarakan masalah keamanan sangatlah luas dan tidak ada habisnya, karena perkembangan masalah keamanan berjalan seiring dengan perkembangan teknologi komputer.

Dalam dunia perkuliahan sering di temui pembelajaran kriptografi hanya membahas teori mengenai kriptografi, hanya membahas tanpa lebih dalam lagi mengenai kriptografi dan tidak bisa mengetahui secara detail dari proses kriptografi yang sedang terjadi. Oleh karena itu, pembelajaran mengenai kriptografi kurang diminati.

Dari uraian tersebut maka penulis bermaksud untuk membuat suatu perangkat lunak sebagai media pembelajaran Kriptografi untuk membantu dalam pembelajaran mengenai beberapa algoritma kriptografi. Dengan alasan tersebut, penulis bermaksud mengajukan penelitian dengan judul "PEMBUATAN PERANGKAT LUNAK sebagai MEDIA PEMBELAJARAN KRIPTOGRAFI ALGORITMA VIGENERE CIPHER dan AES 128bit (*ADVANCED ENCRYPTION STANDARD*)".

1.2 Rumusan Masalah

Berdasarkan latar belakang yang diuraikan di atas, maka dapat dirumuskan pokok permasalahan yang di hadapi yaitu:

1. Bagaimana menganalisa dan mengimplementasikan algoritma kriptografi Vigenere dan *Advanced Encryption Standard* (AES) dalam mendekripsi dan mengenkripsi suatu kata atau kalimat pada Borland Delphi?

1.3 Batasan Masalah

Dalam penyusunan skripsi ini, agar pembahasan tidak terlalu meluas dan untuk memudahkan penyelesaian nantinya, maka dijabarkan beberapa batasan masalah sebagai berikut:

1. Perangkat lunak ini dapat melakukan enkripsi dan dekripsi kata atau kalimat yang diinputkan.
2. Algoritma yang digunakan adalah Algoritma Vigenere dan *Advanced Encryption Standard* (AES).
3. Pembuatan aplikasi dengan Borland Delphi.
4. Input dalam perangkat lunak ini hanya berupa text.

1.4 Tujuan Penelitian

Tujuan dari pembuatan skripsi ini adalah :

1. Skripsi ini dibuat sebagai syarat kelengkapan akademik untuk memperoleh gelar Sarjana S1 di Sekolah Tinggi Manajemen Informatika dan Komputer AMIKOM Yogyakarta.
2. Pembuatan perangkat lunak yang bisa memudahkan dalam pemahaman algoritma Vigenere dan AES.

3. Menghasilkan aplikasi sederhana yang berguna yang dibuat dengan Borland Delphi.

1.5 Manfaat Penelitian

Manfaat penelitian yang dapat diperoleh dari penelitiaan ini adalah sebagai berikut :

1. Penulis
   a. Dapat mengembangkan hasil pikiran dan karyanya, dan berkontribusi dalam penerapan Ilmu Kriptografi dalam kehidupan sehari-hari.
   b. Mampu mencari, mengetahui, menganalisis dan mendata ke dalam bentuk laporan yang tersusun baik dan sistematis.
   c. Memperdalam dan menambah pengalaman Ilmu Pemrograman dan Ilmu Kriptografi.
   d. Menerapkan ilmu yang diperoleh saat menimba ilmu di STMIK AMIKOM Yogyakarta.
2. Akademis
   a. Memudahkan dalam pemahaman algoritma Vigenere dan AES.
   b. Merupakan sumbangan pikiran terhadap ilmu pengetahuan khususnya Ilmu Pemrograman dan Ilmu Kriptografi.
   c. Menambah literatur perpustakaan dan bahan pertimbangan yang berhubungan dengan Skripsi atau tugas akhir.

3. Pembaca

Sebagai referensi bagi yang ingin mengetahui langkah-langkah dari proses enkripsi dan dekripsi serta membagi wawasan tentang Ilmu Pemrograman dan Ilmu Kriptografi.

1.6 Metode Pengumpulan Data

Dalam melakukan penelitian dan pembuatan skripsi ini penulis menggunakan metode-metode penelitian sebagai berikut:

1. Metode literatur

   Metode pengambilan data menggunakan berbagai macam literatur yaitu mencari informasi diberbagai website yang memiliki konten berkaitan dengan dunia kriptografi.

2. Metode kepustakaan

   Metode kepustakaan dengan membaca buku-buku literatur, dokumen, catatan kuliah dan bacaan lainnya sebagai referensi yang berhubungan dengan permasalahan.

1.7 Sistematika Penulisan

Sistematika penulisan adalah gambaran secara keseluruhan dari materi yang akan dibahas dan di uraikan dalam penyusunan laporan ini. Sistematika penulisan laporan pada skripsi adalah sebagai berikut:

BAB I PENDAHULUAN

Bab ini terdiri dari latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, metodologi pengumpulan data, dan sistematika penulisan yang digunakan.

BAB II LANDASAN TEORI

Bab ini berisikan tentang tinjauan pustaka, teori-teori dan software yang mendukung dalam pembuatan penelitian ini.

BAB III ANALISIS DAN PERANCANGAN

Bab ini berisi penjelasan tentang gambaran umum objek penelitian, analisis, rancangan implementasi, dan proses pembuatan aplikasi.

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Bab ini akan menguraikan tentang tahap-tahap peracangan dan pembuatan program perangkat lunak, tentang cara kerja sistem dan pembahasan serta melakukan pengujian aplikasi yang dibuat.

BAB V PENUTUP

Bab ini menyajikan kesimpulan serta saran.